MONOMIAL-LIKE CODES

EDGAR MARTÍNEZ-MORO[1], HAKAN ÖZADAM[2], FERRUH ÖZBUDAK[2], STEVE SZABO[3]

[1] Departamento de Matemática Aplicada
Universidad de Valladolid, Campus Duques de Soria, 42003 Soria, Castilla, Spain
e-mail: edgar@maf.uva.es

[2] Department of Mathematics and Institute of Applied Mathematics
Middle East Technical University, İnönü Bulvarı, 06531, Ankara, Turkey
e-mail: {ozhakan,ozbudak}@metu.edu.tr

[3] Department of Mathematics
Ohio University, Athens, Ohio, 45701, USA
szabo@math.ohiou.edu

Abstract. As a generalization of cyclic codes of length p^s over $\mathbb{F}_{p^a}$, we study n-dimensional cyclic codes of length $p^{s_1} \times \cdots \times p^{s_n}$ over $\mathbb{F}_{p^a}$ generated by a single "monomial". Namely, we study multi-variable cyclic codes of the form $\langle (x_1-1)^{i_1} \cdots (x_n-1)^{i_n} \rangle \subset \frac{\mathbb{F}_q[x_1,\ldots,x_n]}{\langle x_1^{p^{s_1}}-1,\ldots,x_n^{p^{s_n}}-1\rangle}$. We call such codes *monomial-like codes*. We show that these codes arise from the product of certain single variable codes and we determine their minimum Hamming distance. We determine the dual of monomial-like codes yielding a parity check matrix. We also present an alternative way of constructing a parity check matrix using the Hasse derivative. We study the weight hierarchy of certain monomial like codes. We simplify an expression that gives us the weight hierarchy of these codes.

Keywords: Monomial ideal, cyclic code, repeated-root cyclic code, Hamming distance, generalized Hamming weight

1. Introduction

Cyclic codes are said to be repeated-root when the codeword length and the characteristic of the alphabet are not coprime. In some cases repeated-root cyclic codes have the following interesting properties. Massey et. al. have shown in [13] that cyclic codes of length p over a finite field of characteristic p are optimal. There also exist infinite families of repeated-root cyclic codes in even characteristic according to the results of [16]. It was pointed out in [13] that some repeated-root cyclic codes can be decoded using a very simple circuitry. Among the studies on repeated-root cyclic codes are [1], [2], [9], [11], [13], [14] and [16].

Contrary to the simple-root case, there are repeated root cyclic codes of the form $\langle f^i(x)\rangle$ where $i > 1$. Specifically, all cyclic codes of length p^s over a finite field of characteristic p are generated by a single "monomial" of the form $(x-1)^i$, where $0 \le i \le p^s$ (c.f. [2] and [14]). In this paper, as a generalization of these codes to many variables, we study cyclic codes of

the form

$$\langle (x_1-1)^{i_1}\cdots(x_n-1)^{i_n}\rangle \subset \frac{\mathbb{F}_{p^a}[x_1,\ldots,x_n]}{\langle x_1^{p^{s_1}}-1,\ldots,x_n^{p^{s_n}}-1\rangle}.$$

In other words, we study n-dimensional cyclic codes of length $p^{s_1}\times\cdots\times p^{s_n}$, generated by a single "monomial", over a finite field of characteristic p. We call these codes "monomial-like" codes. After exploring some properties of the ambient space $\frac{\mathbb{F}_{p^a}[x_1,\ldots,x_n]}{\langle x_1^{p^{s_1}},\ldots,x_n^{p^{s_n}}\rangle}$, we show that monomial-like codes arise from product codes. More precisely, we show that multi-variable monomial-like codes are actually the product of one-variable monomial-like codes. This enables us to express the minimum Hamming distance of monomial-like codes as a product of the minimum Hamming distance of cyclic codes of length p^s which was computed in [2] and [14]. In addition to this, we determine the dual of monomial-like codes which also yields a parity check matrix for monomial like codes.

The weight hierarchy of linear codes was introduced in [6] and [17]. For some application motives, the weight hierarchy is considered as an important property of a liner code. We simplify an expression, which was conjectured in [18] and proved in [15], for certain monomial like codes. We obtain a simplified expression that gives the weight hierarchy of the monomial like codes which are products of cyclic codes of length p over $\mathbb{F}_{p^a}$.

In [1], the authors show how to construct a parity check matrix for repeated-root cyclic codes in one variable. This construction is based on the Hasse derivative and the repeated-root factor test. When the codeword length is a power of p, their construction applies to monomial-like codes in one variable. We generalize the repeated-root factor test and the construction of the parity check matrix to monomial-like codes in many variables.

This paper is organized as follows. First we introduce some notation, give some definitions and prove some structural properties of the ambient space of monomial-like codes in Section 2. In Section 3, we define monomial-like codes. We show that these codes arise from product codes and we determine their Hamming distance. We describe the dual of monomial-like codes which yields a parity check matrix for these codes. In Section 4, we study the generalized Hamming weight of some product codes and simplify an expression which gives the weight hierarchy of certain monomial-like codes. In Section 5, we explain how to construct a parity check matrix for monomial-like codes using the Hasse derivative.

2. The Ambient Space

Throughout the paper, we consider the finite ring

$$\mathcal{R} = \frac{\mathbb{F}_q[x_1,\ldots,x_n]}{\langle x_1^{p^{s_1}}-1, x_2^{p^{s_2}}-1,\ldots,x_n^{p^{s_n}}-1\rangle} \tag{2.1}$$

as the ambient space of the codes to be studied unless stated otherwise. We define

$$L = \{(i_1,i_2,\ldots,i_n):\quad 0\le i_j < p^{s_j},\quad i_j\in\mathbb{Z}\quad \text{for all}\quad 1\le j\le n\}.$$

The elements of $\mathcal{R}$ can be identified uniquely with the polynomials of the form

$$f(x_1,\ldots,x_n) = \sum_{(i_1,i_2,\ldots,i_n)\in L} f_{(i_1,i_2,\ldots,i_n)} x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},$$

so throughout the paper, we identify the equivalence class $f(x_1,\dots,x_n)+\langle x_1^{p^{s_1}}-1, x_2^{p^{s_2}}-1,\dots,x_n^{p^{s_n}}-1\rangle$ with the polynomial $f(x_1,\dots,x_n)$. The n-dimensional cyclic codes over $\mathbb{F}_q$ of length $p^{s_1}\times p^{s_2}\times\cdots\times p^{s_n}$ are exactly the ideals of $\mathcal{R}$ where we identify each codeword $(f_{(i_1,i_2,\dots,i_n)})_{(i_1,i_2,\dots,i_n)\in L}$ with the polynomial $f(x_1,\dots,x_n)$ via a fixed monomial ordering. The support of $f(x_1,\dots,x_n)$ is the set

$$\mathcal{G}(f)=\{(i_1,i_2,\dots,i_n)\in L:\quad f_{(i_1,i_2,\dots,i_n)}\neq 0\},$$

and the Hamming weight of $f(x_1,\dots,x_n)$ is defined as

$$w_H(f(x_1,\dots,x_n))=|\mathcal{G}(f)|,$$

i.e., the number of nonzero coefficients of $f(x_1,\dots,x_n)$. The minimum Hamming distance of a code C is defined as

$$d_H(C)=\min\{w_H(f(x_1,\dots,x_n)):\quad f(x_1,\dots,x_n)\in C\setminus\{0\}\}.$$

Lemma 2.1. *$\mathcal{R}$ is a local ring with the maximal ideal $M=\langle x_1-1,x_2-1,\dots,x_n-1\rangle$.*

Proof. Let $f(x_1,\dots,x_n)\in\mathcal{R}$. Using the substitution $x_\ell=(x_\ell-1)+1$, for all $1\le\ell\le r$, we can express $f(x_1,\dots,x_n)$ as

$$f(x_1,\dots,x_n)=\sum c_{i_1,i_2,\dots,i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}=\sum d_{i_1,i_2,\dots,i_n}(x_1-1)^{i_1}(x_2-1)^{i_2}\cdots(x_n-1)^{i_n}.$$

If $d_{0,0,\dots,0}\neq 0$, then $f(x_1,\dots,x_n)=f_0(x_1,x_2,\dots,x_n)+d_{0,0,\dots,0}$ for some $f_0(x_1,x_2,\dots,x_n)\in\langle x_1-1,x_2-1,\dots,x_n-1\rangle$. Since $x_\ell-1$ are nilpotent, for all $1\le\ell\le n$, $f_0(x_1,x_2,\dots,x_n)$ is also a nilpotent element and therefore, being a sum of a nilpotent element and a unit, $f(x_1,x_2,\dots,x_n)$ is a unit. In other words, $\mathcal{R}\setminus\{\langle x_1-1,x_2-1,\dots,x_n-1\rangle\}$ consists of exactly the units of $\mathcal{R}$. This implies that $\mathcal{R}$ is a local ring with the maximal ideal $\langle x_1-1,x_2-1,\dots,x_n-1\rangle$. □

Remark 2.2. Not all the ideals of $\mathcal{R}$ are of the form $\langle(x_1-1)^{i_1},\dots,(x_n-1)^{i_n}\rangle$. As a counter-example, we consider

$$\hat{\mathcal{R}}=\frac{\mathbb{F}_q[x,y]}{\langle x^{p^{s_1}}-1,y^{p^{s_2}}-1\rangle},$$

$\hat{I}=\langle x^{p^{s_1}}-1,y^{p^{s_2}}-1\rangle$ and let $J=\langle(x-1)(y-1)\rangle+\hat{I}$. Suppose that there exist $p^{s_1}>m>0$ and $p^{s_2}>n>0$ such that

$$J=\langle(x-1)^m,(y-1)^n\rangle+\hat{I}.$$

Then $(x-1)^m+\hat{I}\in J=\langle(x-1)(y-1)\rangle+\hat{I}$. So, for some $g(x,y)\in\mathbb{F}_q[x,y]$, we have, $(x-1)^m-g(x,y)(x-1)(y-1)\in\hat{I}=\langle x^{p^{s_1}}-1,y^{p^{s_2}}-1\rangle$. Therefore

$$(x-1)^m-g(x,y)(x-1)(y-1)=\alpha_1(x,y)(x-1)^{p^{s_1}}+\alpha_2(x,y)(y-1)^{p^{s_2}}\tag{2.2}$$

for some $\alpha_1(x,y),\alpha_2(x,y)\in\mathbb{F}_q[x,y]$. Evaluating both sides of (2.2) at $y=1$, we get

$$(x-1)^m=\alpha_1(x,1)(x-1)^{p^{s_1}}.$$

This is a contradiction because $m<p^{s_1}$.

Remark 2.3. We have the ring isomorphism

$$\frac{\mathbb{F}_q[x_1,\ldots,x_n]}{\langle x_1^{p^{s_1}}-1, x_2^{p^{s_2}}-1,\ldots,x_n^{p^{s_n}}-1\rangle} \cong \frac{\mathbb{F}_q[y_1,\ldots,y_n]}{\langle y_1^{p^{s_1}}, y_2^{p^{s_2}},\ldots,y_n^{p^{s_n}}\rangle}$$

where the isomorphism is established by sending $x_i - 1$ to y_i.

Let p be an odd prime and let $GR(p^a,m)$ be the Galois ring of characteristic p^a with p^{am} elements. Let N be an odd integer. By [3, Proposition 5.1], we know that the rings

$$\frac{GR(p^a,m)[x]}{\langle x^N-1\rangle} \quad \text{and} \quad \frac{GR(p^a,m)[x]}{\langle x^N+1\rangle}$$

are isomorphic. This is generalized to multi-variable constacyclic codes in the next lemma.

Lemma 2.4. *Let $c_1, c_2, \ldots, c_n \in GR(p^a,m)^*$ be some units of $GR(p^a,m)$. Let $k_1, k_2, \ldots, k_n$ be odd positive integers. The map*

$$\xi : \frac{GR(p^a,m)[x_1,x_2,\ldots,x_n]}{\langle x_1^{k_1}-1, x_2^{k_2}-1,\ldots,x_n^{k_n}-1\rangle} \to \frac{GR(p^a,m)[x_1,x_2,\ldots,x_n]}{\langle x_1^{n_1}-c_1^{k_1}, x_2^{k_2}-c_2^{n_2},\ldots,x_r^{k_r}-c_n^{k_n}\rangle}$$

defined by

$$f(x_1,x_2,\ldots,x_n) \mapsto f(c_1^{-1}x_1, c_2^{-1}x_2,\ldots,c_n^{-1}x_n)$$

is a ring isomorphism.

Proof. Let $I = \langle x_1^{k_1}-1, x_2^{k_2}-1,\ldots,x_n^{k_n}-1\rangle$ and $J = \langle x_1^{k_1}-c_1^{k_1}, x^{k_2}-c_2^{k_2},\ldots,x_n^{k_n}-c_n^{k_n}\rangle$. For every k_i, we have $(c_i^{-1}x_i)^{k_i}-1 = c_i^{-k_i}(x_i^{k_i}-c_i^{k_i})$. Therefore

$$f(x_1,x_2,\ldots,x_n) \equiv g(x_1,x_2,\ldots,x_n) \mod I$$

if and only if there are polynomials $h_e(x_1,x_2,\ldots,x_n), e \in \{1,2,\ldots,n\}$ such that

$$\begin{aligned}
& f(x_1,x_2,\ldots,x_n) - g(x_1,x_2,\ldots,x_n)\\
= \ & h_1(x_1,x_2,\ldots,x_n)(x_1^{k_1}-1)h_2(x_1,x_2,\ldots,x_n)(x_2^{k_2}-1)+\cdots+h_n(x_1,x_2,\ldots,x_n)(x_n^{k_n}-1)
\end{aligned}$$

if and only if

$$\begin{aligned}
& f(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n) - g(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)\\
= \ & h_1(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)((c_1^{-1}x_1)^{k_1}-1)+h_2(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)((c_2^{-1}x_2)^{k_2}-1)\\
& +\cdots+h_r(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)((c_n^{-1}x_n)^{k_n}-1)\\
= \ & h_1(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)c_1^{-k_1}(x_1^{k_1}-c_1^{k_1})+h_2(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)c_2^{-k_2}(x_2^{k_2}-c_2^{k_2})\\
& +\cdots+h_n(c_1^{-1}x_1,c_2^{-1}x_2,\ldots,c_n^{-1}x_n)c_n^{-k_n}(x_n^{k_n}-c_n^{k_n})
\end{aligned}$$

if and only if

$$f(x_1,x_2,\ldots,x_n) \equiv g(x_1,x_2,\ldots,x_n) \mod J.$$

This implies that ξ is well-defined and ξ is injective. The fact that ξ respects addition is obvious. It is also easy to see that

$$\xi(ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}f(x_1,x_2,\ldots,x_n)) = \xi(ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n})\xi(f(x_1,x_2,\ldots,x_n)). \tag{2.3}$$

Together with the fact that ξ is linear, (2.3) implies that $\xi(f(x_1,x_2,\dots,x_n)\cdot g(x_1,x_2,\dots,x_n)) = \xi(f(x_1,x_2,\dots,x_n))\xi(g(x_1,x_2,\dots,x_n))$, for every

$$f(x_1,x_2,\dots,x_n), g(x_1,x_2,\dots,x_n) \in \frac{GR(p^a,m)[x_1,x_2,\dots,x_n]}{\langle x_1^{k_1}-1, x_2^{k_2}-1,\dots,x_n^{k_n}-1\rangle}.$$

Thus ξ is a ring homomorphism. For every

$$h(x_1,x_2,\dots,x_n) \in \frac{GR(p^a,m)[x_1,x_2,\dots,x_n]}{\langle x_1^{k_1}-c_1^{k_1}, x_2^{k_2}-c_2^{k_2},\dots,x_n^{k_n}-c_n^{k_n}\rangle},$$

we have $\xi(h(c_1x_1,c_2x_2,\dots,c_nx_n)) = h(x_1,x_2,\dots,x_n)$. Hence ξ is onto. Thus ξ is an isomorphism. $\square$

Lemma 2.4 tells us that, in our case, we can work with negacyclic codes instead of cyclic codes. More precisely, we have the following corollary.

Corollary 2.5. *The rings*

$$\frac{\mathbb{F}_q[x_1,x_2,\dots,x_n]}{\langle x_1^{p^{s_1}}-1, x_2^{p^{s_2}}-1,\dots,x_n^{p^{s_n}}-1\rangle} \quad \text{and} \quad \frac{\mathbb{F}_q[x_1,x_2,\dots,x_n]}{\langle x_1^{p^{s_1}}+1, x_2^{p^{s_2}}+1,\dots,x_n^{p^{s_n}}+1\rangle}$$

are isomorphic, where the isomorphism is established by sending each x_i to $-x_i$. In even characteristic, these rings are exactly the same.

Thus, for $C_1 = \langle (x_1-1)^{i_1}, (x_2-1)^{i_2},\dots,(x_n-1)^{i_n}\rangle \subset \frac{\mathbb{F}_q[x_1,x_2,\dots,x_n]}{\langle x_1^{p^{s_1}}-1, x_2^{p^{s_2}}-1,\dots,x_n^{p^{s_n}}-1\rangle}$ and $C_2 = \langle (x_1+1)^{i_1}, (x_2+1)^{i_2},\dots,(x_n+1)^{i_n}\rangle \subset \frac{\mathbb{F}_q[x_1,x_2,\dots,x_n]}{\langle x_1^{p^{s_1}}+1, x_2^{p^{s_2}}+1,\dots,x_n^{p^{s_n}}+1\rangle}$, C_1 and C_2 have the same distance distribution and, consequently, have the same minimum Hamming distance.

3. Monomial-like codes

The elements of $\mathbb{F}_q[x_1,\dots,x_n]$ are $\mathbb{F}_q$-linear combinations of monomials $x_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$. From this perspective, one can say that monomials are building blocks of polynomials. Analogously, as a consequence of Lemma 2.1, the elements of $\mathcal{R}$ are $\mathbb{F}_q$-linear combinations of the terms $(x_1-1)^{\alpha_1}(x_2-1)^{\alpha_2}\dots(x_n-1)^{\alpha_n}$, where $(\alpha_1,\dots,\alpha_n)\neq(0,\dots,0)$. So, as was done in [4], we call the terms $(x_1-1)^{\alpha_1}(x_2-1)^{\alpha_2}\dots(x_n-1)^{\alpha_n}$ as "monomials" and ideals generated by monomials as "monomial ideals". "Monomial ideals" of $\frac{\mathbb{F}_q[x_1,\dots,x_n]}{\langle x_1^p-1,\dots,x_n^p-1\rangle}$ were studied in [4]. We concentrate on a special class of monomial ideals that are generated by a single monomial, in a more general ambient space. We call such ideals as "*monomial-like ideals*" and the corresponding codes as "*monomial-like codes*". Namely, monomial-like codes are of the form $C = \langle (x_1-1)^{\alpha_1}(x_2-1)^{\alpha_2}\cdots(x_n-1)^{\alpha_n}\rangle \subset \mathcal{R}$.

Our aim is to determine the minimum Hamming distance of monomial-like codes. Let C be a monomial-like code. In one variable case, the minimum Hamming distance of C was computed in [14] and [2]. It turns out that, in multivariate case, C can be considered as a "product" of single variable codes. This decomposition allows us to express the minimum Hamming distance of C in terms of the Hamming distances of cyclic codes of length p^{s_j}.

Below we define the product of two linear codes. For the general theory of product codes, we refer to [10, Chapter 18].

Definition 3.1. The product of two linear codes $C, C^{'}$ over $\mathbb{F}_q$ is the linear code $C \otimes C^{'}$ whose codewords are all the two dimensional arrays for which each row is a codeword in C and each column is a codeword in $C^{'}$.

Remark 3.2. The following are some well-known facts about the product codes.

(1) If C and $C^{'}$ are $[n, k, d]$ and $[n^{'}, k^{'}, d^{'}]$ codes respectively, then $C \otimes C^{'}$ is a $[nn^{'}, kk^{'}, dd^{'}]$ code.

(2) If G and $G^{'}$ are generator matrices of C and $C^{'}$ respectively, then $G \otimes G^{'}$ is a generator matrix of $C \otimes C^{'}$, where $\otimes$ denotes the Kronecker product of matrices and the codewords of $C \otimes C^{'}$ are seen as concatenations of the rows in arrays in $C \otimes C^{'}$.

First, we prove that, in two variable case, monomial-like codes are product codes.

Theorem 3.3. *Let n_1, n_2 be positive integers and let*

$$\hat{\mathcal{R}} = \frac{\mathbb{F}_q[x, y]}{\langle x^{n_1} - 1, y^{n_2} - 1 \rangle},$$

$$\mathcal{R}_x = \frac{\mathbb{F}_q[x]}{\langle x^{n_1} - 1 \rangle}, \quad \mathcal{R}_y = \frac{\mathbb{F}_q[y]}{\langle y^{n_2} - 1 \rangle}.$$

Suppose that $(x-1)^{k_1} | x^{n_1} - 1$ and $(y-1)^{k_2} | y^{n_2} - 1$. The code $C = \langle (x-1)^{k_1} (y-1)^{k_2} \rangle \subset \hat{\mathcal{R}}$ is the "product" of the codes $C_x = \langle (x-1)^{k_1} \rangle \subset \mathcal{R}_x$ and $C_y = \langle (y-1)^{k_2} \rangle \subset \mathcal{R}_y$, i.e., $C = C_x \otimes C_y$.

Proof. Let

$$\begin{aligned} g(x) &= (x-1)^{k_1} = g_{k_1} x^{k_1} + \cdots + g_1 x + g_0, \\ h(y) &= (y-1)^{k_2} = h_{k_2} y^{k_2} + \cdots + h_1 y + h_0. \end{aligned}$$

Then

$$G_x = \begin{bmatrix} 0 & \ldots & 0 & 0 & g_{k_1} & \ldots & g_1 & g_0 \\ 0 & \ldots & 0 & g_{k_1} & \ldots & g_1 & g_0 & 0 \\ \vdots & & & & & & & \vdots \\ g_{k_1} & \ldots & g_1 & g_0 & 0 & \ldots & 0 & 0 \end{bmatrix},$$

$$G_y = \begin{bmatrix} 0 & \ldots & 0 & 0 & h_{k_2} & \ldots & h_1 & h_0 \\ 0 & \ldots & 0 & h_{k_2} & \ldots & h_1 & h_0 & 0 \\ \vdots & & & & & & & \vdots \\ h_{k_2} & \ldots & h_1 & h_0 & 0 & \ldots & 0 & 0 \end{bmatrix}$$

are two generator matrices for C_x and C_y, respectively. The Kronecker product of G_x and G_y is an $d_1 \cdot d_2 \times n_1 \cdot n_2$ matrix given by

$$G_x \otimes G_y =$$

$$\begin{bmatrix} 0 & 0 & \ldots & 0 & 0 & 0 & g_{k_1}h_{k_2} & g_{k_1}h_{k_2-1} & \cdots & g_{k_1}h_0 & g_{k_1-1}h_{k_2} & \ldots & g_0h_{k_2} & \ldots & g_0h_1 & g_0h_0 \\ 0 & & \ldots & 0 & g_{k_1}h_{k_2} & g_{k_1}h_{k_2-1} & \cdots & g_{k_1}h_0 & g_{k_1-1}h_{k_2} & \ldots & g_0h_{k_2} & \ldots & g_0h_1 & g_0h_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & & & & & & & & & \vdots \\ g_{k_1}h_{k_2} & g_{k_1}h_{k_2-1} & \cdots & g_{k_1}h_0 & g_{k_1-1}h_{k_2} & \ldots & g_0h_{k_2} & \ldots & g_0h_1 & g_0h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

Next, for a polynomial

$$f(x,y) = \sum_{\substack{0 \le i < n_1 \\ 0 \le j < n_2}} c_{ij} x^i y^j \in \mathbb{F}_q[x,y],$$

we use the monomial ordering $x > y$ to order its terms. According to this ordering, we identify $f(x,y)$ with the tuple $(c_{n_1-1,n_2-1}, c_{n_1-1,n_2-2}, \dots, c_{n_1,0}, \dots, c_{n_1-2,n_2-1}, \dots, c_{n_1-2,0}, \dots, c_{0,0})$. Since the elements of $C = \langle (x-1)^{k_1}(y-1)^{k_2} \rangle \subset \hat{\mathcal{R}}$ are exactly all the $\mathbb{F}_q$-linear combinations of the elements of the set

$$\beta = \{x^i y^j (x-1)^{k_1}(y-1)^{k_2} : \quad 0 \le i < n - k_1, \quad 0 \le j < n - k_2\},$$

we obtain a generator matrix for C as

$$G = \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 & 0 & g_{k_1}h_{k_2} & g_{k_1}h_{k_2-1} & \cdots & g_{k_1}h_0 & g_{k_1-1}h_{k_2} & \cdots & g_0h_{k_2} & \cdots & g_0h_1 & g_0h_0 \\ 0 & \cdots & 0 & g_{k_1}h_{k_2} & g_{k_1}h_{k_2-1} & \cdots & g_{k_1}h_0 & g_{k_1-1}h_{k_2} & \cdots & g_0h_{k_2} & \cdots & g_0h_1 & g_0h_0 & 0 & \cdots & 0 \\ \vdots & & & & & & & & & & & & & & & \vdots \\ g_{k_1}h_{k_2} & g_{k_1}h_{k_2-1} & \cdots & g_{k_1}h_0 & g_{k_1-1}h_{k_2} & \cdots & g_0h_{k_2} & \cdots & g_0h_1 & g_0h_0 & 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix}.$$

It is easily seen that $G_x \otimes G_y = G$. Note that in the above construction, we multiplied $(x-1)^{k_1}(y-1)^{k_2}$ with the monomials in the order
$x^0y^0, x^0y^1, x^0y^2, \dots, x^0y^{n-k_2-1}, x^1y^0, \dots, x^1y^{n-k_2-1}, \dots, x^{n-k_1-1}y^0, x^{n-k_1-1}y^1, x^{n-k_1-1}y^{n-k_2-1}$
and considered the corresponding tuples and placed these tuples into G in that order. $\square$

Using the arguments in the proof of Theorem 3.3 inductively, it is straightforward to generalize Theorem 3.3 to the multivariate case.

Theorem 3.4. *Let $r_1, \dots, r_n, i_1, \dots, i_n$ be positive integers and let*

$$\mathcal{R}' = \frac{\mathbb{F}_q[x_1, \dots, x_n]}{\langle x_1^{r_1} - 1, \dots, x_n^{r_n} - 1 \rangle}, \quad \mathcal{R}_{x_j} = \frac{\mathbb{F}_q[x_j]}{\langle x_j^{r_j} - 1 \rangle}.$$

Suppose that $(x_j - 1)^{i_j} | x_j^{r_j} - 1$ for all $1 \le j \le n$. The code

$$C = \langle (x_1 - 1)^{i_1} \cdots (x_r - 1)^{i_r} \rangle$$

is the "product" of the codes $C_{x_j} = \langle (x_j - 1)^{i_j} \rangle \subset \mathcal{R}_{x_j}$, i.e.,

$$C = (\cdots((C_{x_1} \otimes C_{x_2}) \otimes C_{x_3}) \otimes \cdots) \otimes C_{x_n}.$$

Using Theorem 3.4, we determine the minimum Hamming distance of monomial-like codes.

Theorem 3.5. *Let $C = \langle (x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n} \rangle \subset \mathcal{R}$. Let $\mathcal{R}_{x_j} = \frac{\mathbb{F}_q[x_j]}{\langle x^{p^{s_j}} - 1 \rangle}$ and $C_{x_j} = \langle (x_j - 1)^{i_j} \rangle \subset R_{x_j}$. Then $d_H(C) = \prod_{j=1}^n d_H(C_{x_j})$, where $d_H(C_{x_j})$ is as given in* [2, Theorem 6.4] *and* [14, Theorem 1].

Proof. We have $C = (\cdots((C_{x_1} \otimes C_{x_2}) \otimes C_{x_3}) \otimes \cdots) \otimes C_{x_n}$ by Theorem 3.4. The result follows by Remark 3.2 (2). $\square$

3.1. **The dual of monomial-like codes.**

We determine the dual of

$$C = \langle (x_1-1)^{N_1}\cdots(x_n-1)^{N_n}\rangle \subset \frac{\mathbb{F}_q[x_1,\dots,x_n]}{\langle x_1^{p^{s_1}}-1,\cdots,x_n^{p^{s_n}}-1\rangle} = \mathcal{R}.$$

Let $L \subset \mathbb{N}^n$ and $i=(i_1,\dots,i_n)\in L$. We consider $f(x_1,\dots,x_x)\in\mathcal{R}$ in the form

$$f(x_1,\dots,x_n) = \sum_{i\in L} c_i (x_1-1)^{i_1}\cdots(x_n-1)^{i_n}$$

where $c_i \neq 0$, for all $i\in L$. We define

$$\begin{aligned} L_1 &= \{(i_1,\dots,i_n): \quad i_j < p^{s_j}-N_j \quad \forall\, 1\le j\le n\},\\ L_2 &= \{(i_1,\dots,i_n): \quad i_j \ge p^{s_j}-N_j \quad \text{for some} \quad 1\le j\le n\}. \end{aligned}$$

This gives us a partition of L as $L = L_1 \sqcup L_2$. Since

$$(x_1-1)^{N_1}\cdots(x_n-1)^{N_n} f(x_1,\dots,x_n) = (x_1-1)^{N_1}\cdots(x_n-1)^{N_n}\sum_{i\in L_1} c_i(x_1-1)^{i_1}\cdots(x_n-1)^{i_n},$$

we deduce that $(x_1-1)^{N_1}\cdots(x_n-1)^{N_n}f(x_1,\dots,x_n)=0$ if and only if $(x_1-1)^{N_1}\cdots(x_n-1)^{N_n}\sum_{i\in L_1} c_i(x_1-1)^{i_1}\cdots(x_n-1)^{i_n}=0$ if and only if $(x_j-1)^{p^{s_j}-N_j} | f(x_1,\dots,x_x)$ for some $1\le j\le n$. Equivalently, if $f(x_1,\dots,x_n)\in C^\perp$, then $f(x_1,\dots,x_x)\in\langle (x_1-1)^{p^{s_1}-N_1},\dots,(x_n-1)^{p^{s_n}-N_n}\rangle$. Conversely, $(x_j-1)^{p^{s_j}-N_j}(x_1-1)^{N_1}\cdots(x_n-1)^{N_n}=0$ for all $1\le j\le n$. This proves the following.

Lemma 3.6. *Let*

$$C = \langle (x_1-1)^{N_1}\cdots(x_n-1)^{N_n}\rangle \subset \frac{\mathbb{F}_q[x_1,\dots,x_n]}{\langle x_1^{p^{s_1}}-1,\cdots,x_n^{p^{s_n}}-1\rangle}.$$

Then

$$C^\perp = \langle (x_1-1)^{p^{s_1}-N_1},\dots,(x_n-1)^{p^{s_n}-N_n}\rangle.$$

Remark 3.7. Lemma 3.6 does not hold for arbitrary codeword lengths. That is, if

$$\mathcal{R}' = \frac{\mathbb{F}_q[x_1,\dots,x_n]}{\langle x_1^{A_1}-1,\dots,x_n^{A_n}-1\rangle},$$

then since $x_j^{A_j}-1=(x-1)^{A_j}$ only when $A_j=p^{s_j}$ for some s_j, the above arguments are not valid for arbitrary A_j.

Via Lemma 2.4, Lemma 3.6 can be generalized to constacyclic codes.

Lemma 3.8. *Let*

$$D = \langle (x_1-c_1)^{N_1}\cdots(x_n-c_n)^{N_n}\rangle \subset \frac{\mathbb{F}_q[x_1,\dots,x_n]}{\langle x_1^{p^{s_1}}-c_1^{p^{s_1}},\cdots,x_n^{p^{s_n}}-c_n^{p^{s_n}}\rangle}.$$

Then

$$D^\perp = \langle (x_1-c_1)^{p^{s_1}-N_1},\dots,(x_n-c_n)^{p^{s_n}-N_n}\rangle.$$

Now we construct an $\mathbb{F}_q$-basis for $C^\perp$. This also gives us a generator matrix for $C^\perp$ and hence a parity check matrix for C.

We define

$$\begin{aligned} T &= \{(a_1,\ldots,a_n)\in\mathbb{N}^n: \quad p^{s_j}-N_j\le a_j<p^{s_j}\} \quad \text{and}\\ B &= \{(x_1-1)^{a_1}\cdots(x_n-1)^{a_n}: \quad (a_1,\ldots,a_n)\in T\}. \end{aligned}$$

Since the set $B^{'}=\{x_1^{a_1}\cdots x_n^{a_n}: \quad (a_1,\ldots,a_n)\in T\}$ is linearly independent, by the isomorphism given in Remark 2.3, we see that the set B is linearly independent. Let

$$T_j=\{(a_1,\ldots,a_n)\in\mathbb{N}^n: \quad p^{s_j}-N_j\le a_j<p^{s_j}\}.$$

then we can view T as

$$T=T_1\cup\cdots\cup T_n. \tag{3.1}$$

Let $p^s=p^{s_1}\cdots p^{s_n}$. Note that $|T_j|=N_j\frac{p^s}{p^{s_j}}$ moreover,

$$|T_{e_1}\cap\cdots\cap T_{e_r}|=N_{e_1}\cdots N_{e_r}\frac{p^s}{p^{s_{e_1}}\cdots p^{s_{e_r}}}.$$

Now applying the inclusion-exclusion principle to (3.1), we obtain

$$\begin{aligned} |T| &= N_1^{p^s/p^{s_1}}+\cdots+N_n^{p^s/p^{s_n}}-N_1N_2\frac{p^s}{p^{s_1}p^{s_2}}-\cdots-N_{n-1}N_n\frac{p^s}{p^{s_{n-1}}p^{s_n}}+\cdots+(-1)^nN_1\cdots N_n\\ &= p^{s_1}\cdots p^{sNn}-(p^{s_1}-N_1)\cdots(p^{s_n}-N_n). \end{aligned}$$

Clearly $|B|=|T|=p^{s_1}\cdots p^{s_n}-(p^{s_1}-N_1)\cdots(p^{s_n}-N_n)$. On the other hand, we know, from Theorem 3.3, that $\dim(C)=(p^{s_1}-N_1)\cdots(p^{s_n}-N_n)$. This implies that $\dim(C)=p^{s_1}\cdots p^{s_n}-\dim(C)=p^{s_1}\cdots p^{s_n}-(p^{s_1}-N_1)\cdots(p^{s_n}-N_n)$. Therefore the set B is an $\mathbb{F}_q$-basis for $C^{\perp}$. Considering the vector representations of the elements of B, we obtain a generator matrix for $C^{\perp}$ and a parity check matrix for C. In Section 5, we present another method of finding a parity check matrix for C.

In particular, in 2 variable case, there are few enough cases to express B and T more explicitly in a feasible way.

We define

$$\begin{aligned} T^{(2)} &= \{(k,m): \quad p^{s_1-i}\le k<p^{s_1} \quad \text{and} \quad p^{s_2-j}\le m<p^{s_2}\}\\ &\quad \sqcup\{(k,m): \quad 0\le k<p^{s_1-i} \quad \text{and} \quad p^{s_2-j}\le m<p^{s_2}\}\\ &\quad \sqcup\{(k,m): \quad p^{s_1-i}\le k<p^{s_1} \quad \text{and} \quad o\le m<p^{s_2-j}\}. \end{aligned}$$

The set

$$B^{(2)}=\{(x-1)^k(y-1)^m: \quad (k,m)\in T^{(2)}\}$$

is linearly independent and $|T^{(2)}|=p^{s_1}p^{s_2}-(p^{s_1}-i)(p^{s_2}-j)$. Hence $B^{(2)}$ is an $\mathbb{F}_q$-basis for $C_2^{\perp}$.

4. Weight hierarchy of some monomial-like codes

Let

$$\mathcal{R}^{'}=\frac{\mathbb{F}_q[x]}{\langle x^p-1\rangle}$$

and $C = \langle (x-1)^i \rangle \subset \mathcal{R}'$. It was shown in [13, Theorem 5] that C is an MDS code. The weight hierarchy of MDS codes are determined in [8, Theorem 7.10.7]. First we state the weight hierarchy of C and prove it for the sake completeness. Next we study the weight hierarchy of the product of two monomial-like codes which are subsets of $\mathcal{R}'$. For such codes, we simplify an expression that gives us the weight hierarchy of monomial-like codes of the form

$$C_{xy} = \langle (x-1)^i (y-1)^j \rangle \subset \frac{\mathbb{F}_q[x,y]}{\langle x^p - 1, y^p - 1\rangle}. \tag{4.1}$$

We begin by giving the necessary definitions and facts. The reader is referred to [8, Section 7.10] or [12] for the details. The support of a codeword $c = (c_1, \ldots, c_m)$ is the set

$$\chi(c) = \{i : \quad c_i \neq 0\}.$$

The support of a subset $S \subset \mathbb{F}_q^m$ is the set

$$\chi(S) = \bigcup_{c \in S} \chi(c).$$

If $D \subset \mathbb{F}_q^m$ is a subspace of C, then we denote this by $D \leq C$. The r^{th} minimum Hamming weight of a code C is defined as

$$d_r(C) = \min\{\#\chi(D) : D \leq C, \quad \dim(D) = r\}.$$

The weight hierarchy of a k-dimensional code C is the sequence

$$(d_1(C), d_2(C), \ldots, d_k(C)).$$

An easy, yet important, observation is that $d_1(C) = d_H(C)$. To see this, consider the 1-dim subspace of C generated by a minimum weight codeword.

Now we give a lower bound on the generalized Hamming weight of C.

Lemma 4.1. *Let $D \subset C = \langle (x-1)^i \rangle \subset \frac{\mathbb{F}_q[x]}{\langle x^p - 1\rangle}$ be a k-dimensional subspace of C. Then*

$$\chi(D) > i + k - 1.$$

Proof. Assume the converse. Let $\mathcal{B} = \{\beta_1, \ldots, \beta_k\}$ be a basis for D. For

$$\beta_1 = (\beta_{1,1}, \ldots, \beta_{1,p}), \ldots, \beta_k = (\beta_{k,1}, \ldots, \beta_{k,p}),$$

let $e_1, \ldots, e_{i+k-1}$ be the coordinates where $\beta_1, \ldots, \beta_k$ are possibly nonzero. In other words, the generators $\beta_1, \ldots, \beta_k$ (hence all the elements of D) are zero at the coordinates $\{1, 2, \ldots, p\} \setminus \{e_1, \ldots, e_{i+k-1}\}$. For $1 \leq \ell \leq k$, define

$$\beta'_\ell = (\beta_{\ell, e_1}, \ldots, \beta_{\ell, e_{i+k-1}}).$$

Since $\beta_1, \ldots, \beta_k$ are linearly independent, the vectors $\beta'_1, \ldots, \beta'_k$ are also linearly independent. Then, after some rearrangement if necessary, applying Gaussian elimination, we can put these vectors in such a form, say $\alpha_1, \ldots, \alpha_k$, that each α_ℓ has at least $N+(\ell-1)$ leading zeroes where $N \geq 0$. Thus, the vector α_k has at least $k-1$ leading zeroes. So $w_H(\alpha_k) \leq i+k-1-(k-1) = i$. This implies that there is a codeword $\hat{\alpha}_k$, which is obtained after putting back the stripped off zeroes, with $d_H(\hat{\alpha}_k) < i+1$. This is a contradiction because $d_H(C) = i+1$. Hence $\chi(D) > i + k - 1$. $\square$

Using the above lower bound, we determine the generalized Hamming weight of C. We would like to note that the next corollary is an immediate consequence of [8, Theorem 7.10.7].

Corollary 4.2. *Let* $C = \langle (x-1)^i \rangle \subset \frac{\mathbb{F}_q[x]}{\langle x^p - 1\rangle}$. *Then*

$$d_r(C) = i + r.$$

Proof. Since

$$d_r(C) = \min\{\#\chi(D) : \quad D \leq C, \quad \dim(D) = r\},$$

by Lemma 4.1, it suffices to show that there exists an r dimensional subspace D, of C such that $\chi(D) = i + r$. Consider the subspace $T = \langle (x-1)^i, x(x-1)^i, \dots, x^{r-1}(x-1)^i \rangle$. Obviously, the generators are linearly independent and $\dim(T) = r$. It is not hard to see that $\chi(D) = i + 1 + (r-1) = i + r$. This completes the proof. □

Remark 4.3. Corollary 4.2 gives us the weight hierarchy of all cyclic codes of length p over a finite field of characteristic p. With the notation in Corollary 4.2, the weight hierarchy of C is

$$(d_1(C), d_2(C), \dots, d_{p-i}(C)) = (i+1, i+2, \dots, p). \tag{4.2}$$

Using the weight hierarchy of C (4.2), we study the weight hierarchy of codes that are product of cyclic codes of length p over $\mathbb{F}_q$.

A (k_1, k_2)-partition of an integer r is a non-increasing sequence $\pi = (t_1, \dots, t_{k_1})$ such that $t_1 + \cdots + t_{k_1} = r$ and $t_i \leq k_2$ for all $1 \leq i \leq k_1$. We denote all the (k_1, k_2) partitions of r by $P(k_1, k_2, r)$.

Let D_1, D_2 be $[n_1, k_1, d_1], [n_2, k_2, d_2]$ linear codes, respectively. Let

$$\bigtriangledown(\pi) = \sum_{i=1}^{k_1} (d_i(D_1) - d_{i-1}(D_1)) d_{t_i}(D_2), \quad \pi \in P(k_1, k_2, r), \tag{4.3}$$

$$d_r^*(D_1 \otimes D_2) = \min\{\bigtriangledown(\pi) : \quad \pi \in P(k_1, k_2, r)\}.$$

From [15, Theorem 1] , we know that $d_r^*(D_1 \otimes D_2) = d_r(D_1 \otimes D_2)$.

Now, for $C_1 = \langle (x-1)^{i_1} \rangle \subset \frac{\mathbb{F}_q[x]}{\langle x^p - 1\rangle}$ and $C_2 = \langle (y-1)^{i_2} \rangle \subset \frac{\mathbb{F}_q[y]}{\langle y^p - 1\rangle}$, using (4.2), the expression (4.3) simplifies to

$$\begin{aligned} \bigtriangledown(\pi) &= (i_1+1) d_{t_1}(C_2) + \sum_{i=2}^{k_2} d_{t_i}(C_2) \\ &= (i_1+1)(i_2+t_1) + \sum_{i=2}^{k_2} (i_2 + t_i). \end{aligned} \tag{4.4}$$

In the following lemmas, we consider the cyclic codes C_1, C_2 which are as introduced above with the same notation.

Lemma 4.4. *Let* $\pi_0 = (m, t_2, \dots, t_k)$ *be a* (k_1, k_2)*-partition of* r *such that* $\bigtriangledown(\pi_0)$ *is minimum among all* $\bigtriangledown(\hat{\pi})$ *where* $\hat{\pi} \in P(k_1, k_2, r)$. *Then, for the* (k_1, k_2)*-partition* $\pi = (m, m, \dots, m, u, 0, \dots, 0)$ *of* r, *where* $0 < u \leq m$, *we have*

$$\bigtriangledown(\pi_0) = \bigtriangledown(\pi).$$

Proof. Say $\pi = (a_1, \ldots, a_{e-1}, a_e, a_{e+1}, \ldots, a_{k_1})$, where $a_1 = \cdots = a_{e-1} = m$, $a_e = u$ and $a_{e+1} = \cdots = a_{k_1} = 0$. If $\pi = \pi_0$, then we are done. If $a_i = t_i$ for all $1 \le i \le e-1$ and $a_e = u \ge t_e$, then since $\sum_{i=1}^{k_1} a_i = \sum_{i=1}^{k_i} t_i$, we get $u = t_e + t_{e+1} + \cdots + t_{e+\ell}$ for some $\ell \ge 0$. Now, by (4.4), we get

$$\begin{aligned} \bigtriangledown(\pi) &= (i_1+1)(i_2+m) + (e-2)(i_2+m) + (i_2+u), \quad \text{and} \\ \bigtriangledown(\pi_0) &= (i_1+1)(i_2+m) + (e-2)(i_2+m) + \sum_{j=0}^{\ell}(i_2+t_{e+j}). \end{aligned}$$

So, by the minimality of $\bigtriangledown(\pi_0)$, we get $\bigtriangledown(\pi) - \bigtriangledown(\pi_0) = i_2 + u - \sum_{j=0}^{\ell}(i_2 + t_{e+j}) \ge 0$. This implies $\ell = 0$ and $t_e = u$, $t_{e+1} = \cdots = t_{k_1} = 0$. Hence, in this case, $\pi = \pi_0$. If $a_\alpha < t_\alpha = m$ for some $1 < \alpha \le e-1$, then, since π_0 is a non-increasing sequence, π_0 is of the form

$$\pi_0 = (m, m, \ldots, m, t_\alpha, t_{\alpha+1}, \ldots, t_N, 0, \ldots, 0)$$

for some $\alpha + 1 \le N \le k_1$, where $t_j < m$ for all $j \ge \alpha$. This implies that $N \ge e$. So

$$\bigtriangledown(\pi_0) = (i_1+1)(i_2+m) + (\alpha-2)(i_2+m) + \sum_{j=\alpha}^{N}(i_2+t_i).$$

On the other hand,

$$\bigtriangledown(\pi) = (i_1+1)(i_2+m) + (\alpha-2)(i_2+m) + \sum_{j=\alpha}^{e}(i_2+a_i).$$

Since $\sum_{j=\alpha}^{N} t_i = \sum_{j=\alpha}^{e} a_i$, we get

$$\bigtriangledown(\pi) - \bigtriangledown(\pi_0) = (e-\alpha+1)i_2 - (N-\alpha+1)i_2 \ge 0,$$

by the minimality of $\bigtriangledown(\pi_0)$. By the fact that $N \ge e$, we obtain

$$\bigtriangledown(\pi) - \bigtriangledown(\pi_0) = (e-\alpha)i_2 - (N-\alpha)i_2 \le 0.$$

Thus $\bigtriangledown(\pi) = \bigtriangledown(\pi_0)$. □

Lemma 4.5. *Let r be an integer such that $\alpha k_1 < r \le (\alpha+1)k_1$. Let*

$$S = \{(\beta, \beta, \ldots, \beta, u_\beta, 0, \ldots, 0) \in P(k_1, k_2, r) : \quad \alpha + 1 \le \beta \le \min\{k_2, r\}\}.$$

We have

$$d_r(C_1 \otimes C_2) = d_r^*(C_1 \otimes C_2) = d_r(C_1 \otimes C_2) = \min\{\bigtriangledown(\pi) : \quad \pi \in S\}.$$

Lemma 4.5 simplifies the computation of $d_r^*(C_1 \otimes C_2)$ significantly. The search set, for the minimum of $\bigtriangledown(\pi)$, reduces from the set of all (k_1, k_2) partitions of r to the set of (k_1, k_2) partitions of r that are of the form $(\beta, \beta, \ldots, \beta, u_\beta, 0, \ldots, 0)$.

Let C_{xy} be as in (4.1). We know that $C_{xy} = C_1 \otimes C_2$ by Theorem 3.3. Therefore, the above simplification also applies to the generalized Hamming weight of the monomial-like code C_{xy}. More explicitly, we have shown that

$$d_r(C_{xy}) = \min\{\bigtriangledown(\pi) : \quad \pi = (\beta, \beta, \ldots, \beta, u_\beta, 0, \ldots, 0), \quad \pi \in P(k_1, k_2, r)\}.$$

5. Construction of parity check matrix and the Hasse derivative

We begin by recalling the Hasse derivative which is used in the repeated-root factor test. For a detailed treatment of the Hasse derivative, we refer to [5, Chapter 1] and [7, Chapter 5].

The standard derivative for polynomials over a field of positive characteristic, say p, is inappropriate because from the p^{th} derivative on, the result is always zero. For this reason, it is more convenient to work with the Hasse derivative. Sometimes the Hasse derivative is called as the hyper derivative.

Throughout this section, we will use the convention that $\binom{a}{b} = 0$ whenever $b < a$. Let $g(x_1, \ldots, x_n) = \sum d_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n} \in \mathbb{F}_q[x_1, \ldots, x_n]$. The classical derivative of $g(x_1, \ldots, x_n)$ in the direction $(a_1, \ldots, a_n)$ is defined as

$$\frac{\partial^{(a_1+\cdots+a_n)}}{\partial x_1^{a_1} \ldots \partial x_n^{a_n}} g(x_1, \ldots, x_n) = \sum d_{i_1,\ldots,i_n} a_1! \cdots a_n! \binom{i_1}{a_1} \cdots \binom{i_n}{a_n} x_1^{i_1-a_1} \cdots x_n^{i_n-a_n}.$$

The Hasse derivative of $g(x_1, \ldots, x_n)$ in the direction $(a_1, \ldots, a_n)$ is defined as

$$D^{[a_1,\ldots,a_n]}(g(x_1, \ldots, x_n)) = \sum d_{i_1,\ldots,i_n} \binom{i_1}{a_1} \cdots \binom{i_n}{a_n} x_1^{i_1-a_1} \cdots x_n^{i_n-a_n}.$$

We denote the evaluation of $D^{[a_1,\ldots,a_n]}(g(x_1, \ldots, x_n))$ at the point $(\alpha_1, \ldots, \alpha_n)$ by $D^{[a_1,\ldots,a_n]}(g)(\alpha_1, \ldots, \alpha_n)$. We can express $g(x_1, \ldots, x_n)$ as

$$g(x_1, \ldots, x_n) = \sum_{(i_1,\ldots,i_n)\in S} c_{i_1,\ldots,i_n} (x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n}$$

where S is a finite nonempty subset of $\mathbb{N}^n$. Let

$$\begin{aligned} U_\ell &= \{(i_1, \ldots, i_n) \in S : \quad i_\ell \geq m_\ell\}, \\ P_\ell &= \{(i_1, \ldots, i_n) \in S : \quad i_\ell < m_\ell\}. \end{aligned}$$

Obviously $S = U_\ell \sqcup P_\ell$. So

$$\begin{aligned} g(x_1, \ldots, x_n) \quad = & \sum_{(i_1,\ldots,i_n)\in U_\ell} c_{i_1,\ldots,i_n} (x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n} \\ & + \sum_{(i_1,\ldots,i_n)\in P_\ell} c_{i_1,\ldots,i_n} (x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n}. \end{aligned}$$

The term $(x_\ell - 1)^{m_\ell}$ divides $g(x_1, \ldots, x_n)$ if and only if $c_{i_1,\ldots,i_n} = 0$ for all $(i_1, \ldots, i_n) \in P_\ell$. Now suppose that $(x_\ell - 1)^{m_\ell} \nmid g(x_1, \ldots, x_n)$. Then there is $(\hat{i}_1, \ldots, \hat{i}_n) \in P_\ell$ such that $c_{\hat{i}_1,\ldots,\hat{i}_n} \neq 0$. So

$$D^{[\hat{i}_1,\ldots,\hat{i}_n]}(g)(1, \ldots, 1) = c_{\hat{i}_1,\ldots,\hat{i}_n} \binom{\hat{i}_1}{\hat{i}_1} \cdots \binom{\hat{i}_n}{\hat{i}_n} \neq 0.$$

Conversely, if $(x_\ell - 1)^{m_\ell}$ divides $g(x_1, \ldots, x_n)$, then

$$g(x_1, \ldots, x_n) \quad = \sum_{(i_1,\ldots,i_n)\in U_\ell} c_{i_1,\ldots,i_n} (x_1 - 1)^{i_1} \cdots (x_n - 1)^{i_n}.$$

So $D^{[\vec{a}]}(g)(1, \ldots, 1) = 0$ for all $\vec{a} = (a_1, \ldots, a_n)$ with $0 \leq a_\ell < m_\ell$. This proves the following.

Lemma 5.1. *Let $g(x_1,\dots,x_n)\in\mathbb{F}_q[x_1,\dots,x_n]$ and let $A_\ell=\{\vec{a}=(a_1,\dots,a_n)\in\mathbb{N}^n:\quad 0\le a_\ell<m_\ell\}$. Then $(x_\ell-1)^{m_\ell}$ divides $g(x_1,\dots,x_n)$ if and only if $D^{[\vec{a}]}(g)(1,\dots,1)=0$ for all $\vec{a}\in A_\ell$.*

As an immediate consequence, we have the following.

Theorem 5.2. *Let $A_\ell=\{\vec{a}=(a_1,\dots,a_n)\in\mathbb{N}^n:\quad 0\le a_\ell<m_\ell\}$ and $A=\cup_{\ell=1}^n A_\ell$. Let $g(x_1,\dots,x_n)\in\mathbb{F}_q[x_1,\dots,x_n]$. We have $(x_1-1)^{m_1}\cdots(x_n-1)^{m_n}$ divides $g(x_1,\dots,x_n)$ if and only if $D^{[\vec{a}]}(g)(1,\dots,1)=0$ for all $\vec{a}\in A$.*

Let $\mathcal{R}$ be as in (2.1) and let $C=\langle(x_1-1)^{m_1}\cdots(x_n-1)^{m_n}\rangle\subset\mathcal{R}$. We know that $g(x_1,\dots,x_n)\in C$ if and only if $(x_1-1)^{m_1}\cdots(x_n-1)^{m_n}$ divides $g(x_1,\dots,x_n)$. Note that $D^{[a_1,\dots,a_n]}(g)(1,\dots,1)=0$ if $a_\ell\ge p^{s_\ell}$ for some $1\le\ell\le n$. Together with this fact, Theorem 5.2 implies the following.

Theorem 5.3. *Let $C=\langle(x_1-1)^{m_1}\cdots(x_n-1)^{m_n}\rangle\subset\mathcal{R}$. Define $Q_\ell=\{\vec{a}=(a_1,\dots,a_n)\in\mathbb{N}^n:\quad 0\le a_\ell<m_\ell,\quad 0\le a_j<p^{s_j}\quad\text{for}\quad j\ne\ell\}$ and $Q=\cup_{\ell=1}^n Q_\ell$. Then $g(x_1,\dots,x_n)\in C$ if and only if $D^{[\vec{a}]}(g)(1,\dots,1)=0$ for all $\vec{a}\in Q$.*

Fix a monomial order, take $x_1>\cdots>x_n$. Let $\vec{a}=(a_1,\dots,a_n)\in Q$. Consider the vector

$$w_a=\left(\binom{p^{s_1}-1}{a_1}\cdots\binom{p^{s_n}-1}{a_n},\binom{p^{s_1}-1}{a_1}\cdots\binom{p^{s_{n-1}}-1}{a_{n-1}}\binom{p^{s_n}-2}{a_n},\cdots\binom{0}{a_1},\cdots\binom{0}{a_n}\right).$$

For $g(x_1,\dots,x_n)\in\mathcal{R}$, let u_g be the vector representation of the polynomial with respect to the fixed ordering. Then the dot product of w_a and u_g gives us the evaluation of the Hasse derivative of $g(x_1,\dots,x_n)$ at $(1,\dots,1)$ in the direction $\vec{a}$, i.e., $w_a\cdot u_g=D^{[\vec{a}]}(g)(1,\dots,1)$. Now let H be a matrix having rows w_a where $\vec{a}\in Q$ and Q is as in Theorem 5.3. Then H is a parity check matrix for C by Theorem 5.3.

In particular, when there are two variables, we have the following construction. Let

$$\mathcal{R}_2=\frac{\mathbb{F}_q[x,y]}{\langle x^{p^{s_1}}-1,y^{p^{s_2}}-1\rangle}$$

and let $C_2=\langle(x-1)^i(y-1)^j\rangle\subset\mathcal{R}_2$. Define

$$\begin{aligned}A^{(2)}&=\{(k,\ell):\quad 0\le k<k_1\quad\text{and}\quad 0\le\ell<k_2\}\\&\quad\sqcup\{(k,\ell):\quad 0\le k<k_1\quad\text{and}\quad k_2\le\ell<p^{s_2}\}\\&\quad\sqcup\{(k,\ell):\quad k_1\le k<p^{s_1}\quad\text{and}\quad 0\le\ell<k_2\}.\end{aligned}$$

For

$$f(x,y)=\sum_{\substack{0\le i<p^{s_1}\\0\le j<p^{s_2}}}f_{ij}x^iy^j,$$

using the lexicographic order $x>y$, we can view $f(x,y)$ as the vector

$$f=(f_{p^{s_1}-1,p^{s_2}-1},f_{p^{s_1}-1,p^{s_2}-2},\dots,f_{p^{s_1}-1,0},\dots,f_{0,0}).$$

So

$$D^{[k,\ell]}(f)(1,1)=f\cdot\left(\binom{p^{s_1}-1}{k}\binom{p^{s_2}-1}{\ell},\binom{p^{s_1}-1}{k}\binom{p^{s_2}-2}{\ell},\dots,\binom{0}{k}\binom{0}{\ell}\right).$$

Hence an $(ip^{s_2} + jp^{s_1} - ij) \times (p^{s_1} p^{s_2})$ matrix whose rows are

$$\left[\binom{p^{s_1}-1}{k}\binom{p^{s_2}-1}{\ell}, \binom{p^{s_1}-1}{k}\binom{p^{s_2}-2}{\ell}, \ldots, \binom{0}{k}\binom{0}{\ell}\right]$$

where $(k, \ell) \in A^{(2)}$, is a parity check matrix for C_2.

References

[1] Guy Castagnoli, James L. Massey, Philipp A. Schoeller, and Niklaus von Seemann. On repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):337–342, 1991.

[2] Hai Q. Dinh. On the linear ordering of some classes of negacyclic and cyclic codes and their distance distributions. *Finite Fields Appl.*, 14(1):22–40, 2008.

[3] Hai Quang Dinh and Sergio R. López-Permouth. Cyclic and negacyclic codes over finite chain rings. *IEEE Trans. Inform. Theory*, 50(8):1728–1744, 2004.

[4] Vesselin Drensky and Piroska Lakatos. Monomial ideals, group algebras and error correcting codes. In *Applied algebra, algebraic algorithms and error-correcting codes (Rome, 1988)*, volume 357 of *Lecture Notes in Comput. Sci.*, pages 181–188. Springer, Berlin, 1989.

[5] David M. Goldschmidt. *Algebraic functions and projective curves*, volume 215 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2003.

[6] Tor Helleseth, Torleiv Kløve, and Johannes Mykkeltveit. The weight distribution of irreducible cyclic codes with block length $n_1((q^l - 1)/N)$. *Discrete Math.*, 18(2):179–211, 1977.

[7] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres. *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics. Princeton University Press, Princeton, NJ, 2008.

[8] W. Cary Huffman and Vera Pless. *Fundamentals of error-correcting codes*. Cambridge University Press, Cambridge, 2003.

[9] Sergio R. López-Permouth and Steve Szabo. On the Hamming weight of repeated root cyclic and negacyclic codes over Galois rings. *Adv. Math. Commun.*, 3(4):409–420, 2009.

[10] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes. I*. North-Holland Publishing Co., Amsterdam, 1977. North-Holland Mathematical Library, Vol. 16.

[11] E. Martínez-Moro and I. F. Rúa. On repeated-root multivariable codes over a finite chain ring. *Des. Codes Cryptogr.*, 45(2):219–227, 2007.

[12] Conchita Martínez-Pérez, Hans Georg Schaathun, and Wolfgang Willems. On weight hierarchies of product codes. The Wei-Yang conjecture and more. In *International Workshop on Coding and Cryptography (Paris, 2001)*, volume 6 of *Electron. Notes Discrete Math.*, page 7 pp. (electronic). Elsevier, Amsterdam, 2001.

[13] James L. Massey, Daniel J. Costello, and Jørn Justesen. Polynomial weights and code constructions. *IEEE Trans. Information Theory*, IT-19:101–110, 1973.

[14] Hakan Özadam and Ferruh Özbudak. A note on negacyclic and cyclic codes of length p^s over a finite field of characteristic p. *Adv. Math. Commun.*, 3(3):265–271, 2009.

[15] Hans Georg Schaathun. The weight hierarchy of product codes. *IEEE Trans. Inform. Theory*, 46(7):2648–2651, 2000.

[16] J. H. van Lint. Repeated-root cyclic codes. *IEEE Trans. Inform. Theory*, 37(2):343–345, 1991.

[17] Victor K. Wei. Generalized Hamming weights for linear codes. *IEEE Trans. Inform. Theory*, 37(5):1412–1418, 1991.

[18] Victor K. Wei and Kyeongcheol Yang. On the generalized Hamming weights of product codes. *IEEE Trans. Inform. Theory*, 39(5):1709–1713, 1993.